Franchise Tax Board

2007 National Automated Clearing House Association (NACHA) **Audit**

EXECUTIVE SUMMARY

Physical and System Access Violations May Go Undetected!

In accordance with the *NACHA Operating Rules* for Internet-Initiated Entries, the Internal Audit Section has conducted an audit of Internet-initiated taxpayer payments to ensure there are proper protections in place to safeguard sensitive taxpayer information. The FTB Web Pay and e-Installment Agreements (eIA) payment programs are currently the two FTB programs that provide taxpayers with the option of making payments via the Web. Accordingly, this audit was conducted in order to assure that these programs utilize appropriate security practices and procedures.

Nothing came to our attention, based on the work performed, that would indicate that FTB security standards and practices did not adequately protect financial information obtained from taxpayers over the Internet. However, we identified two areas where we recommend that security controls be strengthened in order to provide a greater deterrent against security violations. These are reflected in the chart below.

	Finding	Recommendation
F1	Department of General Services (DGS) staff that are assigned to work at the FTB do not undergo Department of Justice (DOJ) background checks.	Internal Audit recommends that DGS staff working at the FTB undergo DOJ background checks to provide greater assurance that FTB equipment and taxpayer information is adequately safeguarded.
F2	The monitoring of eGateway Systems security logs is inadequate.	Internal Audit recommends that the Information Security Audit Unit: ▪ Develop and adhere to timetables for their plan to develop meaningful audit reports for the eGateway Systems. ▪ Audit the eGateway Systems access logs on a regular basis so that unacceptable user activites can be detected in a timely manner that allows for the prevention of repeated access violations and misuse of taxpayer bank information.

The detail of these findings can be found in Appendix A.

Auditee Response

The Privacy, Security & Disclosure Bureau concurred with the recommendations contained in this report and has provided Internal Audit with a plan of action (POA) for implementation. The details of the POA can be found in Appendix B.

State of California
Franchise Tax Board

11.18.2008

To: Denise Mellor, Director
Privacy, Security & Disclosure Bureau

From: Philip Yu

2007 National Automated Clearing House Association (NACHA) Audit for Internet Initiated Payments

Physical and System Access Violations May Go Undetected!

Memorandum

The Franchise Tax Board (FTB), Internal Audit Section, has completed its 2007 annual NACHA Audit for Internet-Initiated Payments.

Introduction

In accordance with the *NACHA Operating Rules* for Internet-Initiated Entries, the Internal Audit Section has conducted an audit of Internet-initiated taxpayer payments to ensure there are proper protections in place to safeguard sensitive taxpayer information. The FTB Web Pay and e-Installment Agreements (eIA) payment programs are currently the two FTB programs that provide taxpayers with the option of making payments via the Web. Accordingly, this audit was conducted in order to assure that these programs utilize appropriate security practices and procedures.

Background

The FTB Web Pay Program allows taxpayers the opportunity to request an electronic debit to their bank account for the purpose of making a single online payment against their personal income tax debt. For periodic payments against outstanding tax bills, the FTB eIA program allows taxpayers to setup an online installment agreement. To initiate a Web Pay or eIA payment, taxpayers must provide their social security number and last name in order to verify their identity. After specifying a payment amount and payment terms, taxpayers must authorize the debit to their bank account via a "Web click", which asserts agreement to the payment terms designated by the FTB.

The Originating Depository Financial Institutions (ODFIs) that transmit Internet-initiated debits must warrant that their customers who originate the entries have met security standards, including an annual audit. FTB is considered an "Originator" under *NACHA Operating Rules*, and therefore, must conduct annual audits to assure proper security practices are being followed. As banks can be held liable for losses that result from a failure of their Originators to meet security standards, they have an interest in the outcome of the audits. The State's ODFI is Union Bank. At the completion of the annual audit, FTB certifies to the Bank that appropriate security practices are in place. The *NACHA Operating Rules* require that consumer (taxpayer) financial information obtained by an Originator is protected by security

practices that include adequate levels of: 1) physical security to protect against theft, tampering, or damage, 2) personnel and access controls to protect against unauthorized access and use, and 3) network security to ensure secure capture, storage, and distribution of financial information.

Scope & Objectives

The scope and objective of this audit was to assure that adequate levels of security were in place for taxpayer Web-initiated payments made through the FTB WebPay and eIA programs for the period January 2007 to June 2008. Specifically, our objective was to provide the Department with reasonable assurance that taxpayer financial information obtained via the Web was protected by adequate levels of physical security, personnel and access controls, and network security. The scope of the audit did not include verifying the accuracy of payment processing; therefore, no testing of payment results was performed.

Methodology

In conducting our audit we employed the following methodology:

- Conducted interviews with key individuals within the Filing Division, Technology Services Division, Administration Services Division, and Finance and Executive Services Division to obtain information on the security processes in place;
- Reviewed process and procedural documentation for understanding and accuracy;
- Gathered evidence to substantiate compliance with stated policy and procedures; and
- Performed limited testing procedures around access controls.

Results

Nothing came to our attention, based on the work performed, that would indicate that FTB security standards and practices did not adequately protect financial information obtained from taxpayers over the Internet. However, we identified two areas where we recommend that security controls be strengthened in order to provide a greater deterrent against security violations. These are reflected in the chart below.

	Finding	Recommendation
F1	Department of General Services (DGS) staff that are assigned to work at the FTB do not undergo Department of Justice (DOJ) background checks.	Internal Audit recommends that DGS staff working at the FTB undergo DOJ background checks to provide greater assurance that FTB equipment and taxpayer information is adequately safeguarded.
F2	The monitoring of eGateway Systems security logs is inadequate.	Internal Audit recommends that the Information Security Audit Unit: ▪ Develop and adhere to timetables for their plan to develop meaningful audit reports for the eGateway Systems. ▪ Audit the eGateway Systems access logs on a regular basis so that unacceptable user activites can be detected in a timely manner that allows for the prevention of repeated access violations and misuse of taxpayer bank information.

The detail of these findings can be found in Appendix A.

Conclusion

Based on our review, we concluded that internal controls were sufficient to meet the stated objectives for the period January 2007 through June 2008, except for the findings indicated above.

We have attached the Privacy, Security & Disclosure Bureau response, which adequately addresses the findings and recommendations stated in our report. We concur with your plan of action. Please inform Internal Audit, in writing, of your efforts to implement these actions after 60-days, 6-months, and 1-year from the date of this report. The information you provide us will be used to determine the need for a follow-up review.

We greatly appreciate the cooperation and assistance provided to us by your staff during the 2007 NACHA Audit. We look forward to working in collaboration with the Privacy, Security & Disclosure Bureau and the other bureaus impacted by Internet-initiated taxpayer payments in the next NACHA Audit. If you have any questions or comments, please contact Cynthia Speth at 845-5840.

Philip Yu, Director
Internal Audit Bureau

Attachment

cc: S. Stanislaus
L. Iwafuchi
C. Cleek
L. Crowe
A. Miller
C. Beach
M.Mason
C. Meraji
B. Mills
V. Kotowski
C. Quandt

APPENDIX A

FINDINGS & RECOMMENDATIONS

FINDING 1 (F-1): **Department of General Services (DGS) staff that are assigned to work at the FTB do not undergo Department of Justice (DOJ) background checks.**

CONDITION: All potential FTB employees and vendors undergo a thorough screening by the FTB personnel office. The screening process includes a DOJ background check. An exception exists with DGS staff who are assigned to work at the FTB (maintenance staff, janitorial staff, building engineers, etc.). They do not undergo DOJ background checks before they are permitted on-site to service FTB facilities, including Special Security Areas (SSAs) within our facilities. Currently, even vendors employed by DGS are required to go through background checks, yet the DGS staff person escorting them is not required to do the same.

There are five agencies that are located on-site at the FTB Campus with DGS being the smallest. Worksite Security reported that there were a significant number of security incidents involving DGS personnel, such as parking violations, badge violations, possession of drugs, being under the influence of drugs, and theft. The frequency of incidents increased significantly when DGS changed their cleaning schedule to after-business hours. There were 88 incidents during the fiscal year 7/1/07 – 6/30/08, eleven of which were security breaches. Some of those breaches involved inappropriate access to SSAs.

During the audit period there were two non-DGS security incidents that involved potential identity theft that were short-circuited as a result of DOJ background checks. These incidents, although not perpetrated by DGS personnel, highlight how background checks prevented potentially significant violations to FTB information security.

1) In 2005 FTB hired a temporary employee in the Information Validation Section where she was provided with TI system access. Shortly after being hired the employee became the subject of an investigation by local law enforcement for Social Security Number fraud and tax scams. Law enforcement authorities were able to identify through a DOJ check that this individual worked for FTB and contacted the Department, which led to her dismissal. Years later in February 2008, the High Tech Crime Unit of the CHP contacted the Department to inform us that they found this employee's old FTB badge in the possession of a friend of the ex-FTB employee. The friend also had in his possession other items associated with identity theft.

2) An FTB job applicant, later discovered to be part of an identity theft ring, was denied employment due to failing her DOJ background check on a misdemeanor conviction. The law enforcement agent who informed FTB of the applicant's involvement in an identity theft ring, indicated that individuals who are part of such operations often try to gain employment at a place where they can steal personal information, with that being their sole purpose for seeking employment.

(FINDING 1 (F-1) CON'T)

CRITERIA: General Procedures Manual 9415 states:

> In our commitment to provide an environment of individual responsibility and integrity, candidates seeking employment with FTB are subject to a background investigation. The investigation will include completion of a pre-employment questionnaire and fingerprint card.
>
> If, prior to employment, the candidates are found to be unsuitable for the position for which they indicated interest, their names will be withheld from the eligible list or, in cases of transfer and reinstatement, the job offer will be rescinded.
>
> If, after employment, inconsistencies are identified between information provided by candidates and that provided by the Criminal Investigation and Information (CI&I) Report, they will be removed from employment.

EFFECT: Inappropriate access to FTB information and information systems may occur as a result of having employees from other state agencies on-site who have not undergone background checks as a prevention against criminal activity.

Although DGS personnel are not granted authorized system access, someone with high tech criminal intent could circumvent a background check by gaining access to FTB databases as a DGS employee.

CAUSE: This situation has occurred due to interdepartmental agreements with other state agencies that do not adhere to the same level of stringency in their hiring security practices.

RECOMMENDATION: Internal Audit recommends that DGS staff working at the FTB undergo DOJ background checks in order to provide greater assurance that FTB equipment and taxpayer information is adequately safeguarded.

Note: *FTB senior management is currently exploring the feasibility of making DOJ background checks a condition of DGS staff working at the FTB. They seek to implement this requirement as an added security measure to protect FTB physical and information assets.*

FINDING 2 (F-2): **The monitoring of eGateway Systems security logs is inadequate.**

CONDITION: The eGateway Systems store a history of Internet-initiated WebPay and eIA transaction data. Once stored in eGateway, the information can be accessed through the FTB Intranet. Security logs that track everyone who accesses the Intranet applications write out to a centralized security database known as the Security Audit Log (SAL).

The Information Security Audit Unit (ISAU) utilizes SAL to monitor user access. High-volume usage systems such as TI and ARCS have priority and are monitored/audited on a monthly basis; however, eGateway accesses are reviewed only when questionable accesses are detected through one of these routine audits, or through a special request audit. In addition, ISAU does not have any automated reports for the eGateway Systems, and without meaningful audit reports it is difficult to isolate access violations.

CRITERIA: The FTB Information Security Policy (FTB Policy 9500), Section 605, Monitoring System Access, requires that system usage be monitored as follows:

> Procedures must be established for monitoring the use of information processing facilities. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk analysis. Areas that should be considered for monitoring access include:
>
> - User ID;
> - Date and time of key events;
> - Types of events;
> - Files accessed;
> - Programs/utilities used;
> - All privileged operations, such as: use of supervisor account, system start-up and stop, and I/O device attachment/ detachment;
> - Unauthorized access attempts, such as: failed attempts, access policy violations, gateways and firewalls, and alerts from proprietary intrusion detection systems;
> - System alerts or failures, such as: console alerts or messages, system log exceptions, and network management alarms.
>
> The result of the monitoring activities must be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:
>
> - Criticality of the application processes;
> - Value, sensitivity, or criticality of the information involved;
> - Past experience of system infiltration and misuse;
> - Extent of system interconnection, particularly to public networks.

(FINDING 2 (F-2) CON'T)

EFFECT: Inadequate monitoring of the eGateway Systems compromises protection of taxpayer information. And, in light of the fact that the eGateway stores highly confidential bank account and routing number information, there is an increased risk exposure if misuse were to occur.

Unless inappropriate access is detected in one of the high priority systems that are audited on a routine basis, or through an "on-request" audit, unacceptable user activities within the eGateway Systems may go undetected. The lack of routine monitoring increases the risk of taxpayer bank account information being used for improper purposes. In addition, if such activity were to occur, it could expose the FTB to potential lawsuits.

CAUSE: With limited resources, the ISAU was not able to develop meaningful audit reports for the younger eGateway Systems and monitor them routinely because other high-volume usage systems held a higher monitoring priority.

RECOMMENDATION: At the end of our field work for this audit, ISAU has indicated that they requested and were able to obtain new programmer positions that were filled after the 2008/09 Budget passed. We recognize that with these additional resources, ISAU is currently developing automated reports for the eGateway Systems and that they expect to be able to begin routine audits on eGateway by early next year.

In light of this, we recommend that the ISAU:

- Develop and adhere to timetables for their plan to develop meaningful audit reports for the eGateway Systems.
- Audit the eGateway Systems access logs on a regular basis so that unacceptable user activities can be detected in a timely manner that allows for the prevention of repeated access violations and misuse of taxpayer bank information.

APPENDIX B

RESPONSES TO RECOMMENDATIONS

State of California
Franchise Tax Board

11.14.08

To: Philip Yu, Director
Director Internal Audit Bureau

From: Denise Mellor

Response to 2007 National Automated Clearing House Association (NACHA) Audit for Internet Initiated Payments

Memorandum

This memo is the Privacy, Security and Disclosure Bureau's (PSDB) response to the 2007 National Automated Clearing House Association (NACHA) Audit for Internet Initiated Payments. We agree with the findings and offer the following responses.

Finding 1 (F-1) Department of General Services (DGS) staff that are assigned to work at the FTB do not undergo Department of Justice (DOJ) background checks.

Response: We have been working to resolve this issue for approximately four years. In fact on September 10, 2004, I sent a letter to DGS requesting that their employees that work in FTB buildings go through the DOJ background checks. At that time, we were told they had requests from more that just FTB and would be pursuing our request from a global perspective. We have continued to pursue this request over the years and will continue until such time as we achieve compliance with our request. In the meantime, we are evaluating the feasibility of limiting the hours DGS staff are allowed to work in the buildings. Specifically, for most DGS staff we are exploring the option of limiting their work hours to 6:00 am to 6:00 PM.

Finding 2 (F-2) The monitoring of eGateway System Security logs is inadequate.

Response: As noted in the recommendation we have filled our new positions and were able to develop the proactive audit reports for the eGateway Systems. The reports are now included in our routine monthly audit cycle. The results of the first audit reports are currently under review and have already resulted in at least two potential unauthorized accesses.

Privacy, Security and Disclosure Bureau MS A190
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.5427
fax 916.845.0417
ftb.ca.gov

Thank you for performing the audit. We welcome opportunities to strengthen the protections needed to safeguard sensitive taxpayer information.

Denise Mellor, CSO/Director
Privacy, Security and Disclosure Bureau

State of California
Franchise Tax Board

04.06.09

To: Philip Yu, Director
Internal Audit Bureau

From: Denise Mellor

Update: 60-day and 6-month Response to 2007 National Automated Clearing House Association (NACHA) Audit for Internet Initiated Payments

Memorandum

This memo is the Privacy, Security and Disclosure Bureau's (PSDB) 60-day and 6-month response to the 2007 National Automated Clearing House Association (NACHA) Audit for Internet Initiated Payments. We agree with the findings and offer the following updated responses.

Finding 1 (F-1) Department of General Services (DGS) staff that are assigned to work at the FTB do not undergo Department of Justice (DOJ) background checks.

Response: We have been working to resolve this issue for approximately four years. In fact on September 10, 2004, I sent a letter to DGS requesting that their employees that work in FTB buildings go through the DOJ background checks. At that time, we were told they had requests from more that just FTB and would be pursuing our request from a global perspective. We have continued to pursue this request over the years and will continue until such time as we achieve compliance with our request. In the meantime, we are evaluating the feasibility of limiting the hours DGS staff are allowed to work in the buildings. Specifically, for most DGS staff we are exploring the option of limiting their work hours to 6:00 am to 6:00 PM.

60-day and 6-month Response: I recently met with DGS representatives in the Office of Building and Property Management and the Labor Relations and Program Improvement areas. While they have agreed to consider limiting the hours of some staff, they are concerned about completing all of the work required between 6:00 am and 6:00 PM. In addition, they agreed to work with us to have DGS staff located at FTB go through the Department of Justice Criminal History checks. They have cautioned us that while they have been successful initiating criminal history checks in some organizations, it was a long process and that we should not expect immediate results.

Privacy, Security and Disclosure Bureau MS A190
PO Box 1468
Sacramento CA 95812-1468

tel 916.845.5427
fax 916.845.0417
ftb.ca.gov

Finding 2 (F-2) The monitoring of eGateway System Security logs is inadequate.

Response: As noted in the recommendation, we have filled our new positions and were able to develop the proactive audit reports for the eGateway Systems. The reports are now included in our routine monthly audit cycle. The results of the first audit reports are currently under review and have already resulted in at least two potential unauthorized accesses.

60-day and 6-month Response: As previously reported, the eGateway System audit reports are now included in our routine monthly audit cycle which means the reports are generated and reviewed each month. We believe we have completely addressed the finding to develop meaningful audit reports and audit on a regular basis. We hope that you concur that this item can be considered closed.

We again thank you for performing the audit and look forward to the continuing opportunities to strengthen the protections needed to safeguard sensitive taxpayer information.

Denise Mellor

CSO/Director
Privacy, Security and Disclosure Bureau